UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

i2 INC., a Delaware corporation; and i2 LIMITED, a British limited company registered in England and Wales,

Plaintiffs,

v.

PALANTIR TECHNOLOGIES, INC., a Delaware corporation; SHYAM SANKAR, an individual; DR. ASHER SINENSKY, an individual; SRS ENTERPRISES, LLC, a Florida limited liability company; and NOCHUR SANKAR, an individual,

Defendants.

Civil Action No. 1:10-cv-00885-LO-JFA

PALANTIR TECHNOLOGIES, INC., a Delaware corporation,

Counter-Plaintiff,

v.

i2 INC., a Delaware corporation; and i2 LIMITED, a British limited company registered in England and Wales,

Counter-Defendants.

PALANTIR TECHNOLOGIES, INC.'S ANSWER AND COUNTERCLAIM

Defendant Palantir Technologies, Inc. ("Palantir" or "Defendant") hereby answers the Complaint of Plaintiffs i2, Inc. and i2 Limited (collectively, "i2") as follows:

INTRODUCTION

1. Denied.

2. Palantir lacks knowledge or information sufficient to form a belief as to the truth of the allegations in Paragraph 2 and on that basis denies them.

3. Palantir admits that it is, in some ways, a competitor of i2. Palantir admits that it develops analysis software sold to intelligence, defense, and law-enforcement organizations. Palantir admits that its marketing materials promote its software as "a child of PayPal, born from the start up's methodology for combating fraud." Palantir denies the remainder of the allegations in Paragraph 3.

4. Palantir admits that Shyam Sankar joined Palantir as Director of Business Development in or about March 2006. Palantir admits that Shyam Sankar contacted i2 about purchasing i2 products for SRS Enterprises and that Shyam Sankar was a member of SRS Enterprises since in or before 2004. Palantir admits that Mr. Sankar was interested in i2 products that could be used for commercial fraud investigations. Palantir denies the remainder of the allegations in Paragraph 4.

5. Palantir admits that SRS Enterprises purchased i2's Analyst's Notebook version 6 software and related technical support. Palantir admits that Shyam Sankar was Palantir's Director of Business Development and also a member of SRS Enterprises. Palantir denies the remainder of the allegations in Paragraph 5.

6. This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir lacks sufficient information to admit or deny the allegations in this paragraph, and on that basis denies those allegations.

7. Sentences one and two of this paragraph state legal conclusions to which no response is required, but to the extent a response is required, Palantir lacks sufficient information to admit or deny the allegations in this paragraph, and on that basis denies those allegations. Sentences three and four of this paragraph also state legal conclusions to which no response is

required, but to the extent a response is required, Palantir denies the remainder of these allegations.

8. Palantir denies the allegations in sentence one of this paragraph. Sentence two of this paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir lacks sufficient information to admit or deny the remaining allegations in this sentence, and on that basis denies those allegations. Palantir lacks sufficient information to admit or deny the allegations in sentences three and four, and on that basis denies those allegations. Palantir denies the allegations in sentence five of this paragraph.

9. Palantir admits that i2 makes the contention stated in the last sentence of Paragraph 9, but denies that i2's contentions are true. Palantir admits that Analyst's Notebook Import and iBaseCrawl offer Palantir's customers a way to import the customers' data into Palantir's products. Palantir denies the remainder of the allegations in Paragraph 9.

10. Denied.

11. Palantir admits that i2 seeks the relief described in this paragraph, but denies that i2 is entitled to this relief or any other relief prayed for in its Complaint.

PARTIES

12. Palantir lacks knowledge or information sufficient to form a belief as to the truth of the allegations in Paragraph 12 and on that basis denies them.

13. Palantir lacks knowledge or information sufficient to form a belief as to the truth of the allegations in Paragraph 13 and on that basis denies them.

14. Palantir admits the allegations in sentences one, two, and three, and further admits that Palantir sells certain of its analysis software to intelligence, defense, and law-enforcement agencies, and that Palantir and i2 compete with respect to the sale of certain products. Palantir denies the remainder of the allegations in this paragraph.

15. Palantir admits that SRS Enterprises, LLC has a registered address of 2336 Rye Grass Lane, Oviedo, Florida. Palantir lacks knowledge or information sufficient to form a belief as to the truth of the allegations regarding the records of the Florida Secretary of State, and on that basis denies them. This paragraph contains numerous legal conclusions to which no response is required. Palantir denies the remainder of the allegations in Paragraph 15.

16. Palantir admits that Shyam Sankar is an individual who resides in Palo Alto, California, and that he is an employee of Palantir. Palantir admits that Shyam Sankar joined Palantir as Director of Business Development in or around March 2006 and that he currently holds the title "Director of Forward Deployed Engineering." Palantir admits that Shyam Sankar was a member of SRS enterprises from 2004 or earlier up until 2010. Palantir admits that Shyam Sankar regularly travels to Virginia as part of his duties for Palantir. Palantir denies the remainder of the allegations in Paragraph 16.

17. Palantir admits that Nochur Sankar is an individual who resides at 2336 Rye Grass Lane, Oviedo, Florida, and that he is the father of Shyam Sankar and Ravi Sankar. Palantir admits that Ravi Sankar has been a member of SRS Enterprises. Palantir admits that Ravi Sankar worked as a summer intern at Palantir and that he did work in an engineering capacity, including for the business development team. Palantir admits that Nochur Sankar has been a managing member of SRS Enterprises. Palantir denies the remainder of the allegations in Paragraph 17.

18. Palantir admits the allegations in sentence one of Paragraph 18. Palantir admits that Dr. Sinensky is employed by Palantir as a Forward Deployed Engineer. Palantir denies the remaining allegations of Paragraph 18.

19. This paragraph states legal conclusions to which no response is required.

20. This paragraph states legal conclusions to which no response is required, but to

the extent a response is required, Palantir denies the remainder of the allegations in Paragraph 20.

GENERAL ALLEGATIONS

21. Palantir admits that it has taken an approach to intelligence and law-enforcement data with some similarities to that which Paypal took in the field of electronic payment. Today, as well as in 2006, Palantir continues to develop its software products and continues to provide those products to intelligence agencies. Palantir denies the remaining allegations in Paragraph 21.

22. Palantir admits that Shyam Sankar began his employment at Palantir in or around March 2006 and that his initial position with Palantir was Director of Business Development. Palantir denies the remainder of the allegations in Paragraph 22.

23. Palantir admits that Shyam Sankar began his employment with Palantir in or around March 2006, and that Mr. Sankar contacted i2 and asked for information. Palantir admits that Shyam Sankar's personal email address was ss298@cornell.edu, that he provided this personal email address to i2 as contact information, and that he had attended Cornell University. Palantir admits that Shyam Sankar provided i2 with an address in California and that he received i2 marketing materials at that address. Palantir lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in Paragraph 23 and on that basis denies them.

24. Palantir admits that Shyam Sankar contacted i2 in the spring of 2006 regarding purchasing software capable of being used for commercial fraud investigations. Palantir admits that 2336 Rye Grass Lane, Oviedo, Florida is the registered address for SRS Enterprises and that Shyam Sankar provided this address to i2. Palantir lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in Paragraph 24 and on that basis denies

them.

25. Palantir lacks knowledge or information sufficient to form a belief as to the truth of the allegations in Paragraph 25 and on that basis denies them.

26. Palantir admits that i2 makes the contentions stated in the last sentence of Paragraph 26, but denies that i2's contentions are true. Palantir lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in Paragraph 26 and on that basis denies them.

27. Palantir admits that Nochur Sankar paid for a purchase from i2 on or about April 13, 2006 using an American Express credit card. The final sentence in Paragraph 27 states a legal conclusion to which no response is required, but to the extent a response is required, Palantir denies the allegations in this sentence. Palantir lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in Paragraph 27 and on that basis denies them.

28. Palantir admits that Shyam Sankar, while employed at Palantir, registered for and attended a portion of an i2 user conference on or around May 31, 2006, that he provided his home address and mobile phone number, and identified the company "Xoom." Palantir denies the remaining allegations in Paragraph 28.

29. Palantir lacks knowledge or information sufficient to form a belief as to the truth of the allegations in Paragraph 29 and on that basis denies them.

30. Palantir lacks knowledge or information sufficient to form a belief as to the truth of the allegations in Paragraph 30 and on that basis denies them.

31. This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir lacks knowledge or information sufficient to form a belief as to the truth of the allegations in Paragraph 31 and on that basis denies them.

(a) This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir denies Plaintiffs' characterization of the alleged 2006 license agreement and states that the terms of the alleged license agreement speak for themselves.

(b) This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir denies Plaintiffs' characterization of the alleged 2006 license agreement and states that the terms of the alleged license agreement speak for themselves.

(c) This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir denies Plaintiffs' characterization of the alleged 2006 license agreement and states that the terms of the alleged license agreement speak for themselves.

(d) This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir denies Plaintiffs' characterization of the alleged 2006 license agreement and states that the terms of the alleged license agreement speak for themselves.

(e) This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir denies Plaintiffs' characterization of the alleged 2006 license agreement and states that the terms of the alleged license agreement speak for themselves.

(f) This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir denies Plaintiffs' characterization of the alleged 2006 license agreement and states that the terms of the alleged license agreement speak for themselves.

(g) This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir denies Plaintiffs' characterization of the alleged 2006 license agreement and states that the terms of the alleged license agreement speak for

themselves.

(h) This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir denies Plaintiffs' characterization of the alleged 2006 license agreement and states that the terms of the alleged license agreement speak for themselves.

(i) This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir denies Plaintiffs' characterization of the alleged 2006 license agreement and states that the terms of the alleged license agreement speak for themselves.

(j) This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir denies Plaintiffs' characterization of the alleged 2006 license agreement and states that the terms of the alleged license agreement speak for themselves.

(k) This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir denies Plaintiffs' characterization of the alleged 2006 license agreement and states that the terms of the alleged license agreement speak for themselves.

32. Denied.

33. Palantir admits that i2 sold Nochur Sankar and SRS Enterprises a license to i2's iBase SSE Designer software in or about January 2007, along with one year of technical support, and that the address given for this purchase was 2336 Rye Grass Lane, Oviedo, Florida. Palantir lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in Paragraph 33 and on that basis denies them.

34. Palantir admits that Shyam Sankar contacted i2 to request that certain i2 dongles be consolidated, that Shyam Sankar emailed i2 on or about August 28, 2007, from his email

address, ssankar@gmail.com, and that the email was signed "Thanks, Nochur." Palantir lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in Paragraph 34 and on that basis denies them.

35. This paragraph states a legal conclusion to which no response is required, but to the extent a response is required, Palantir denies the allegations in Paragraph 35.

36. This paragraph states a legal conclusion to which no response is required, but to the extent a response is required, Palantir denies the allegations in Paragraph 36.

37. Denied.

38. Palantir denies the allegations in sentences one, two, and three of this paragraph. Sentence four of this paragraph states a legal conclusion to which no response is required, but to the extent a response is required, Palantir denies the allegations in this sentence.

39. This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir denies the allegations in Paragraph 39.

40. Palantir admits that Dr. Asher Sinensky's email address is asherks@gmail.com and that he has been a Forward Deployed Engineer for Palantir since in or around mid-2007. Palantir lacks knowledge or information sufficient to form a belief as to the truth of the remainder of the allegations in Paragraph 40 and on that basis denies them.

JURISDICTION AND VENUE

41. This paragraph states a legal conclusion to which no response is required.

42. This paragraph states a legal conclusion to which no response is required.

43. This paragraph states a legal conclusion to which no response is required.

44. This paragraph states a legal conclusion to which no response is required.

45. This paragraph states a legal conclusion to which no response is required.

CLAIM I
(Fraud and Conspiracy to Commit Fraud)
(Against Palantir, Shyam Sankar,
SRS Enterprises and Nochur Sankar)

46. Palantir incorporates by reference its responses to Paragraphs 1 through 46, above, as if set forth in full herein.

47. Denied.

48. Denied.

49. The terms of the alleged 2006 license agreement speak for themselves. Palantir denies the remainder of the allegations in Paragraph 49.

50. Denied.

51. Denied.

52. Denied.

53. Denied.

54. Denied.

CLAIM II
(Breach of Contract)
(Against SRS Enterprises, and Alter Ego defendant Shyam Sankar and Nochur Sankar)

55. Palantir incorporates by reference its responses to Paragraphs 1 through 54, above, as if set forth in full herein.

56. This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir lacks knowledge or information sufficient to form a belief as to the truth of the allegations in Paragraph 56 and on that basis denies them.

(a) This paragraph states a legal conclusion to which no response is required, but to the extent a response is required, Palantir states that the terms of the alleged 2006 license speak for themselves and denies the remainder of the allegations in this paragraph.

(b) This paragraph states a legal conclusion to which no response is required,

but to the extent a response is required, Palantir states that the terms of the alleged 2006 license speak for themselves and denies the remainder of the allegations in this paragraph.

(c) This paragraph states a legal conclusion to which no response is required, but to the extent a response is required, Palantir states that the terms of the alleged 2006 license speak for themselves and denies the remainder of the allegations in this paragraph.

(d) This paragraph states a legal conclusion to which no response is required, but to the extent a response is required, Palantir states that the terms of the alleged 2006 license speak for themselves and denies the remainder of the allegations in this paragraph.

(e) This paragraph states a legal conclusion to which no response is required, but to the extent a response is required, Palantir states that the terms of the alleged 2006 license speak for themselves and denies the remainder of the allegations in this paragraph.

(f) This paragraph states a legal conclusion to which no response is required, but to the extent a response is required, Palantir states that the terms of the alleged 2006 license speak for themselves and denies the remainder of the allegations in this paragraph.

(g) This paragraph states a legal conclusion to which no response is required, but to the extent a response is required, Palantir states that the terms of the alleged 2006 license speak for themselves and denies the remainder of the allegations in this paragraph.

(h) This paragraph states a legal conclusion to which no response is required, but to the extent a response is required, Palantir states that the terms of the alleged 2006 license speak for themselves and denies the remainder of the allegations in this paragraph.

(i) This paragraph states a legal conclusion to which no response is required, but to the extent a response is required, Palantir states that the terms of the alleged 2006 license speak for themselves and denies the remainder of the allegations in this paragraph.

57. This paragraph states a legal conclusion to which no response is required, but to

the extent a response is required, Palantir states that the terms of the alleged licenses speak for themselves and denies the remainder of the allegations in this paragraph.

58. Denied.

59. Denied.

60. Denied.

CLAIM III
(Misappropriation Of Trade Secrets)
(Against All Defendants)

61. Palantir incorporates by reference its responses to Paragraphs 1 through 60, above, as if set forth in full herein.

62. Denied.

63. Denied.

64. The terms of the alleged 2006 License Agreement speak for themselves. Palantir denies the remainder of the allegations in this paragraph.

65. Palantir lacks knowledge or information sufficient to form a belief as to the truth of the allegations in Paragraph 65 and on that basis denies them.

66. This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir denies the allegations in Paragraph 66.

67. Denied.

68. Denied.

69. Denied.

70. Denied.

71. Denied.

CLAIM IV
(Copyright Infringement – 17 U.S.C. §§ 501 et seq.)
(Against All Defendants)

72. Palantir incorporates by reference its responses to Paragraphs 1 through 71,

above, as if set forth in full herein.

73. This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir lacks knowledge or information sufficient to form a belief as to the truth of the allegations in Paragraph 73 and on that basis denies them.

74. Palantir admits that the document attached as Exhibit A to Plaintiffs' Complaint purports to be a copy of a certificate of copyright registration for Analyst's Notebook version 7.0. Palantir lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in Paragraph 74 and on that basis denies them.

75. Palantir admits that the document attached as Exhibit B to Plaintiffs' Complaint purports to be a copy of a certificate of copyright registration for iBase version 5.0. Palantir lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in Paragraph 75 and on that basis denies them.

76. Palantir admits that the document attached as Exhibit C to Plaintiffs' Complaint purports to be a copy of a certificate of copyright registration for Analyst's Notebook version 8.0. Palantir lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in Paragraph 76 and on that basis denies them.

77. This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir lacks knowledge or information sufficient to form a belief as to the truth of the allegations in Paragraph 77 and on that basis denies them.

78. This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir lacks knowledge or information sufficient to form a belief as to the truth of the allegations in Paragraph 78 and on that basis denies them.

79. This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir lacks knowledge or information sufficient to form a

belief as to the truth of the allegations in Paragraph 79 and on that basis denies them.

80. Denied.

81. Denied.

82. Denied.

83. Denied.

84. Denied.

85. Denied.

86. Denied.

87. Denied.

88. Denied.

CLAIM V
(Contributory Copyright Infringement)
(Against Defendants SRS Enterprises LLC, Shyam Sankar, And Nochur Sankar)

89. Palantir incorporates by reference its responses to Paragraphs 1 through 88, above, as if set forth in full herein.

90. This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir denies the allegations in Paragraph 90.

91. This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir denies the allegations in Paragraph 91.

92. Denied.

93. Denied.

94. Denied.

CLAIM VI
(Civil RICO--Violation of Title 18 United States Code Section 1962(c))
(Against All Defendants)

95. Palantir incorporates by reference its responses to Paragraphs 1 through 94,

above, as if set forth in full herein.

96. This paragraph states a legal conclusion to which no response is required.

97. Denied.

- **The Enterprise**

98. This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir denies the allegations in Paragraph 98.

99. This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir denies the allegations in Paragraph 99.

100. This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir denies the allegations in Paragraph 100.

101. This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir denies the allegations in Paragraph 101.

102. This paragraph states a legal conclusion to which no response is required, but to the extent a response is required, Palantir denies the allegations in Paragraph 102.

- **Pattern of Racketeering Activity**

103. Denied.

104. Denied.

- **Mail Fraud**

105. Denied.

106. This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir denies the allegations in Paragraph 106.

107. The first sentence of this paragraph states a legal conclusion to which no response is required, but to the extent a response is required, Palantir denies the allegations in this sentence. Palantir lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in Paragraph 107 and on that basis denies them.

108. Palantir denies the allegations in the first two sentences of this paragraph. Palantir lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in Paragraph 108 and on that basis denies them.

109. This paragraph states legal conclusions to which no response is required, but to the extent a response is required, Palantir denies the allegations in Paragraph 109.

- **Wire Fraud**

110. Denied.

111. Denied.

112. Denied.

- **Criminal Infringement of a Copyright**

113. Denied

114. Denied.

- **Direct Injury to i2's Business or Property**

115. Denied.

116. Denied.

CLAIM VII
(Conspiracy To Injure Another In Trade Or Business (Va. Code §§ 18.2-499(A) & 500)
(Against Defendants Palantir, Shyam Sankar,
Nochur Sankar and Dr. Asher Sinensky)

117. Palantir incorporates by reference its responses to Paragraphs 1 through 116, above, as if set forth in full herein.

118. Denied.

119. Denied.

120. Denied.

121. Denied.

RESPONSE TO PRAYER FOR RELIEF

122. Palantir denies that Plaintiffs are entitled to any of the relief they have requested

in paragraphs one through nine of their prayer for relief, and deny all factual allegations contained therein.

123. Palantir denies each allegation of the Complaint not expressly admitted herein and denies that Plaintiffs are entitled to any of the relief requested in the Complaint.

AFFIRMATIVE DEFENSES

FIRST AFFIRMATIVE DEFENSE

(Unclean Hands)

124. Plaintiffs' claims in this case are barred by Plaintiffs' own misconduct under the equitable doctrine of unclean hands. Through methods of the sort that i2 has alleged Defendants employed to obtain confidential and trade secret information, including by infiltrating Palantir's presentations to its users, i2 has sought and obtained the same or similar information about Palantir's products in an effort to unfairly compete with Palantir.

125. i2 brings this lawsuit accusing Palantir of engaging in clandestine means to obtain confidential and trade secret information about i2's products. As alleged in Paragraphs 157 through 192 below, however, behind i2's allegations against Palantir, and arising directly out of the same facts, is a pattern of conduct by i2 that is far worse and far more damaging than the conduct i2 has alleged against Palantir. As alleged in greater detail in Paragraphs 157 through 192, which Paragraphs are hereby incorporated by reference, i2 is pursuing a business strategy of "locking in" its customers' data, thereby preventing Palantir and other software suppliers from delivering interoperable products to intelligence and law-enforcement agencies. By doing so, as further alleged in Paragraphs 157 through 192, i2 has deliberately and intentionally undermined the ability of intelligence and law-enforcement agencies to comply with federal law and policy.

126. Recent fraudulent and deceitful activities of i2 in connection with the Los Angeles County Sheriff's Department ("LASD"), a mutual customer of i2 and Palantir, provide additional support for Palantir's unclean hands defense. i2 appears to have used a company called

Knowledge Computing Corp. ("KCC") in order to gain access to Palantir's confidential information. In or about September 2008, KCC approached Palantir about collaborating on a presentation to the 115th International Association of Chiefs of Police ("IACP"). The idea was to present an integration of the two companies' respective products. The IACP presentation was successful, and in the weeks that followed, Palantir and KCC began discussing a possible joint marketing arrangement. These discussions bore fruit, and on or about December 10, 2008, KCC and Palantir entered into a Co-Marketing Agreement (the "CMA"). The CMA remains in force to this day.

127. Section 1(c) of the CMA provides, *inter alia*, that (i) "[e]ach party shall comply with good business practices and all applicable laws and regulations," (ii) "[d]uring the term hereof, neither party will market, promote, sell, lease, solicit, or procure orders for or otherwise represent any product that is competitive with any of the other party's products," and (iii) "[e]ach party shall conduct its business in a manner that favorably reflects upon the other party and the other party's products." In addition, Section 5 of the CMA, a confidentiality clause, barred KCC from disclosing Palantir's confidential information to any third party without the prior written consent of Palantir.

128. At the time they entered into the CMA, KCC's flagship product was Coplink, a law-enforcement database product. Prior to entering into the CMA, executives of Palantir and KCC entered into a non-disclosure agreement dated September 12, 2008 (the "NDA") and held extensive discussions about integrating and jointly marketing Coplink along with Palantir's software. During these discussions, under the protections of the NDA, Palantir disclosed to KCC highly confidential business information, including information concerning Palantir's marketplace strategies, customer sites where Palantir's software is deployed, and its outlook regarding data integrators.

129. In the months following their execution of the CMA, unbeknownst to Palantir, KCC was engaged in corporate merger discussions with i2. In July of 2009, i2 announced a merger with KCC (the "Merger"). As the surviving company, i2, by operation of law, became the successor in interest to all rights and obligations of KCC under the CMA and the NDA.

130. Despite LASD's strong desire to integrate Coplink and Palantir so that it could make use of data saved in files on Coplink using Palantir's powerful analytical tools, KCC and i2 together, and then i2, alone, following the Merger, erected impediments and roadblocks to the completion of the planned integration. When LASD insisted upon completion of the integration, i2 charged LASD $55,000. In effect, i2 charged LASD $55,000 so that LASD could have access to its own data for importation into Palantir's system.

131. Even though i2 charged LASD for access to its own data, i2 did not in fact give LASD sufficient access to all of the data it sought. Instead, it only permitted integration with a portion of the data – demanding even more money for full integration. The $55,000 charge to LASD was a holdup opportunity that i2 created for itself through its anticompetitive obstruction of a client's desire for interoperability with Palantir. It demonstrates, concretely, that i2's campaign to block its clients' interoperability with Palantir has no legitimate business purpose and does not serve to deliver a better quality product to customers, but rather is being carried out to lessen competition and suppress innovation.

132. In an effort to help LASD with a workaround solution, Palantir expended significant amounts of time and resources modifying the software it had delivered to LASD so that LASD could make effective use of its legacy data. These increased costs eroded the profits Palantir would have earned had the planned integration with Coplink taken place, thus resulting in direct economic loss to Palantir.

133. KCC had a duty to disclose its pending merger discussions with i2. Knowledge

of the pending merger was material, since Palantir, at minimum, could have acted to protect itself by demanding return of its confidential business information prior to consummation of the Merger, before that information fell into i2's hands. Despite this obligation, KCC stood mute.

134. On information and belief, Palantir avers that, at the time the CMA was signed, KCC did not in fact intend to honor its obligations under the CMA and that, then, or at some point prior to the Merger, KCC began acting as a plant for i2 to gain access to Palantir's confidential business information. Had Palantir known the truth, it never would have entered into discussions with KCC, never would have revealed any confidential business information to KCC, and never would have entered into the CMA. By deceit and artifice, KCC and i2 shielded the fact that the Merger was in the works and disclosed nothing until the Merger was announced publicly. Through this deception, KCC and the surviving i2 entity obtained access to Palantir's strategic planning information, particularly with respect to integration with other software tools such as i2, which information i2 could then use to unfairly and unlawfully compete with Palantir.

135. As a result of Plaintiffs' conduct, Plaintiffs' claims are barred by the doctrine of unclean hands.

SECOND AFFIRMATIVE DEFENSE

(Necessity)

136. Plaintiffs' Complaint fails to state any cause of action against Palantir in that any alleged conduct in this case was necessary, in whole or in part, to safeguard national security.

THIRD AFFIRMATIVE DEFENSE

(Failure to State a Claim)

137. Plaintiffs' Complaint fails to state any claim upon which relief can be granted.

FOURTH AFFIRMATIVE DEFENSE

(Proximate Cause)

138. Plaintiffs' claims are barred because Palantir's acts or omissions, wrongful or

otherwise, were not the proximate cause of any of Plaintiffs' alleged injuries, if any.

FIFTH AFFIRMATIVE DEFENSE

(Failure to Mitigate)

139. Assuming without conceding that the Complaint states a claim, Plaintiffs have failed to mitigate their damages, if any.

SIXTH AFFIRMATIVE DEFENSE

(Statute of Limitations)

140. To the extent Plaintiffs seek damages for alleged conduct outside the relevant statutes of limitations for their various claims, Plaintiffs' claims are barred.

SEVENTH AFFIRMATIVE DEFENSE

(Fair Use)

141. Plaintiffs' claims are barred, in whole or in part, by the doctrine of fair use.

EIGHTH AFFIRMATIVE DEFENSE

(Copyright Misuse)

142. Plaintiffs' claims are barred, in whole or in part, by the doctrine of copyright misuse.

NINTH AFFIRMATIVE DEFENSE

(Laches)

143. Plaintiffs' claims are barred by the doctrine of laches.

TENTH AFFIRMATIVE DEFENSE

(License)

144. Plaintiffs' claims are barred, in whole or in part, because Plaintiffs have licensed Defendants' and/or third parties' use of Plaintiffs' technology, and the conduct attributed to Defendants falls within the scope of those licenses.

ELEVENTH AFFIRMATIVE DEFENSE

(Limited Remedies)

145. Assuming without conceding that the Complaint states a claim, Plaintiffs' remedies are limited by the terms of the alleged license agreements.

TWELFTH AFFIRMATIVE DEFENSE

(Justification)

146. Plaintiffs' Complaint fails to state any cause of action against Palantir in that any purported misconduct in this case was done, in whole or in part, to safeguard national security, and Defendants were justified in engaging in the conduct attributable to them.

THIRTEENTH AFFIRMATIVE DEFENSE

(Estoppel)

147. Plaintiffs are estopped, in whole or in part, from asserting the claims alleged and obtaining the relief requested in the Complaint by reason of Plaintiffs' conduct, actions and communications to others.

FOURTEENTH AFFIRMATIVE DEFENSE

(Preemption)

148. Plaintiffs' common law claims are barred, in whole or in part, on the ground that they conflict with, and are preempted by, statute, including but not limited to the Virginia Uniform Trade Secrets Act ("VUTSA") and the Virginia Uniform Computer Information Transactions Act ("VUCITA"), and by public policy.

FIFTEENTH AFFIRMATIVE DEFENSE

(Waiver)

149. Plaintiffs have waived, in whole or in part, any rights they may have to institute an action for the alleged wrongdoings of which they complain by reason of Plaintiffs' conduct, actions and communications to others.

SIXTEENTH AFFIRMATIVE DEFENSE

(Adequate Remedy at Law)

150. Plaintiffs are not entitled to injunctive relief because any alleged injury to Plaintiffs is not immediate or irreparable and Plaintiffs have an adequate remedy at law.

SEVENTEENTH AFFIRMATIVE DEFENSE

(Speculative Damages)

151. Plaintiffs' claims are barred, in whole or in part, because Plaintiffs' alleged damages, if any, are speculative and uncertain.

EIGHTEENTH AFFIRMATIVE DEFENSE

(Consent)

152. Plaintiffs' claims are barred, in whole or in part, because Plaintiffs consented to and approved some of the actions and transactions complained of in the Complaint. Accordingly, Plaintiffs are barred from pursuing damages for those actions.

NINETEENTH AFFIRMATIVE DEFENSE

(Lack of Subject Matter Jurisdiction)

153. This Court lacks subject matter jurisdiction to adjudicate Plaintiffs' state-law claims.

TWENTIETH AFFIRMATIVE DEFENSE

(Failure to State Facts Sufficient To Support Exemplary Damages)

154. Plaintiffs' Complaint fails to state facts sufficient to constitute a claim for exemplary damages. Plaintiffs' claims for exemplary damages are further barred to the extent that such claims are violations of the Fifth, Eighth, and Fourteenth Amendments to the United States Constitution.

COUNTERCLAIM

155. This Court has jurisdiction pursuant to 28 U.S.C. § 1367 because the claims

pleaded in this Counterclaim are so related to the Complaint that they form part of the same case or controversy under Article III of the United States Constitution.

156. The Court has personal jurisdiction over i2, Inc. and i2 Limited because they are present in this District and have availed themselves of this Court's jurisdiction. Venue over the Counterclaim is proper in this District under 28 U.S.C. § 1391(b) because i2, Inc. and i2 Limited are present in this District, because a substantial part of the conduct alleged in the counterclaim occurred in this District, and because a substantial part of the resulting harm has occurred and will continue to occur in this District.

INTRODUCTION

157. The vast majority of Palantir's and i2's customers are United States intelligence agencies, law-enforcement departments, counter-terrorism groups, special forces, and others who collect and analyze mountains of data to protect national security interests and to fight crime. It is "mission critical" for these customers to share information fluidly within their organizations, with soldiers and agents in the field, with other agencies around the country, and with allies around the world. Lives depend on this.

158. Putting its pecuniary interests over the public interest, i2 has attempted to "lock in" data that its customers save using i2's software, thereby depriving those customers of the ability to transfer their own data to a format useable with the software of i2's competitors, including Palantir. Whenever a customer saves any data using i2's software, i2 contends that it may use license restrictions and technical impediments to prevent Palantir from helping that customer transfer the data into a form readable by software other than i2's software so that it may be used with Palantir's software. i2's efforts to "lock in" its customers' data in this way are contrary to federal law and policy.

159. In the aftermath of September 11th, Congress, by statute, and the President, by

executive order, established a national policy requiring that defense, intelligence, and law-enforcement agencies share information freely so that our soldiers, intelligence analysts, and law-enforcement officials can "connect the dots" when handling the increasingly complex types of information with which they are confronted. Central to this federal mandate is a set of prescribed technology standards that require digital information to be stored by government agencies in an open file format so that it may be freely and readily readable by the vast array of differing governmental computer systems. Palantir's and i2's customers have thus demanded data transferability, not as a matter of convenience, but to make effective use of their own data, to meet their obligations under federal law, and to carry out their vital national security missions.

160. In the Answer and the defenses pleaded therein, Palantir responds to the allegations made in the Complaint directly, on the merits. This Counterclaim frames for decision a closely related set of issues arising out of i2's efforts to block the transferability of data across its customers' different software platforms. These issues will surface in some of the defenses Palantir presents, but do not fully overlap with those defenses and are of such distinct and independent importance as to warrant a request for relief on their own terms. By this Counterclaim, Palantir seeks a judicial declaration that (i) it is lawful and permissible for Palantir to enable customers of i2 that have lawfully obtained a license from i2 to transfer their data between i2's software and any other software, including Palantir's, and (ii) any license restriction in i2's customer licenses upon which i2 seeks to rely to block Palantir from assisting customers in this way is null and void.

161. The Counterclaim is ripe for decision and presents a justiciable controversy. The position taken by i2 in this lawsuit that its customer license agreements restrict customers from sharing with i2's competitors i2's "confidential software and related trade secrets and confidential information," Complaint ¶ 31, creates a judicially cognizable dispute between i2 and

Palantir because, if i2's licenses are enforceable in the manner that i2 claims they are, these license restrictions will prevent Palantir and other competitors of i2 – as well as i2 itself – from offering software capable of meeting federally-mandated standards, will obstruct government agencies from meeting their obligations under federal law, and will undermine critically important governmental data-sharing policies.

162. As would any party to a commercial controversy over which this Court has jurisdiction, Palantir is entitled to declaratory relief addressing the disputed rights and obligations of Palantir and i2. Because the transferability issues raised here have national security implications going far beyond the commercial interests of i2 and Palantir, declaratory relief is especially warranted.

A. Federal law and policy mandate an "Information Sharing Environment" among agencies at all levels of government.

163. i2 pursues a business model based on a closed system architecture, preventing customers with data that they have saved using an i2 application from transferring that data to other software. Unlike i2, Palantir uses open data formats. Companies using open data formats enable customers freely to transfer their information by using file formats that can be read by other software products. For example, data stored in a document created using the most recent version of Microsoft Word may be opened with or transferred to non-Microsoft programs with ease. The creator may not only transfer the set of words used, but also the way in which those words have been put together – i.e. the sentences, paragraphs, and document format. In technical terms, this ability to share data between software programs is most commonly called "interoperability," and sometimes in the government context, "data transferability," "data portability," or "data independence."

164. Generally, in the ordinary business setting – at least absent antitrust violations or

other commercial abuses – the law favors neither open nor closed system architectures. But the law is not neutral in the intelligence and law-enforcement sectors. Interoperability is required. After an in-depth examination of the circumstances that led to the September 11th catastrophe, the Final Report of the National Commission on Terrorist Attacks Upon the United States (the "9/11 Report") found that barriers to information sharing among governmental agencies were a critical weakness in our nation's ability to fight terror. In response to this finding, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004 ("IRTPA"), P.L. 108-458 (December 17, 2004), as amended, P.L. 110-53 (August 3, 2007).

165. The IRTPA directs the President to create something called an Information Sharing Environment ("ISE") spanning all levels of government – federal, state and local. The ISE is an information handling infrastructure that "provides and facilitates the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector." 6 U.S.C § 485(b)(2). The IRTPA describes the attributes of the ISE in great detail. *See* 6 U.S.C § 485(b)(2)(A)-(K). Not only is connectivity between different types of technology used by government entities – including, specifically, the integration of older, legacy technologies such as i2's with newer software platforms such as Palantir's – specifically required by the ISE, the statute lists at least a half dozen other "mission critical" attributes for the ISE. *See id.* § 485(b)(2)(A) (ISE must "connect[] existing systems … and allow[] users to share information among agencies, between levels of government, and, as appropriate, with the private sector"); *id.* § 485(b)(2)(C) (ISE must promote "availability of information in a form and manner that facilitates its use in analysis, investigations and operations"); *id.* § 485(b)(2)(D) (ISE must "build[] upon existing systems capabilities currently in use"); *id.* § 485(b)(2)(F) (ISE must "facilitate[] the sharing of information at and across all levels of security"); *id.* § 485(b)(2)(J) (ISE must "integrate[] the information within the scope of the information sharing environment,

including any such information in legacy technologies"); *id.* § 485(b)(2)(L) (ISE must "allow[] the full range of analytic and operational activities without the need to centralize information within the [ISE]").

166. Many of these mission-critical requirements of the IRTPA cannot be feasibly implemented across the entire ISE without the type of open data formats and open platform architecture Palantir provides, and that i2 is deliberately attempting to block. The potential for harm to the national interest is real and immediate. To date, two Presidents have announced that improved intra-governmental information sharing is among our highest national security priorities. *See* National Security Strategy, President Barack Obama (May 2010) ("To prevent acts of terrorism on American soil, we must enlist all of our intelligence, law enforcement, and homeland security capabilities…. We are improving information sharing and cooperation by linking networks to facilitate federal, state and local capabilities to seamlessly exchange messages and information, conduct searches, and collaborate."); National Strategy for Information Sharing, President George W. Bush (October 2007) ("Improving information sharing in the post September 11 world requires an environment that supports the sharing of information across all levels of government, disciplines, and security domains.").

1. The ISE and the PM-ISE

167. The IRTPA created two centers of authority within the executive branch to oversee and implement the creation of the ISE, and both have adopted clear policy directives that mandate interoperability. First, responsibility for exercising Presidential authority to create the ISE resides in a Program Manager for ISE ("PM-ISE"). U.S.C § 485(f). The PM-ISE serves as the Chairman of an interagency group known as the Information Sharing Council ("ISC"), on which the heads of affected civil and defense agencies sit. The ISC has the mission of, *inter alia*, "provid[ing] advice and information concerning the establishment of an interoperable terrorism

information sharing environment to facilitate automated sharing of terrorism information among appropriate agencies…." Executive Order 1338 (October 25, 2005). Among the PM-ISE's duties is the responsibility to develop and adopt "government wide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE."

168. As part of the Common Information Sharing Standards Program ("CISS"), the PM-ISE has adopted common technical standards to be followed within the ISE. Common Terrorism Program Standards Manual, Version 1.0 (October 2007); ISE Enterprise Architectural Framework, Version 2.0 (September 2008); ISE Profile And Architecture Implementation Strategy, Version 2.0 (June 2009). To facilitate cross-platform sharing of information, compliance with the CISS common technical standards requires and would not be feasible without open data formats. The CISS includes a number of initiatives, including the Universal Core ("UCORE") and the National Information Exchange Model ("NIEM"), specifying the software architectures that all agencies must utilize. The UCORE and the NIEM specifically require and depend upon open data formats such as extensible markup language ("XML") or its equivalent.

169. The PM-ISE's common technical standards extend to the state and local levels. For example, a network of Fusion Centers receives law-enforcement information from a variety of sources, including federal, state and local entities. Fusion Centers ensure that law-enforcement offices within their geographic areas of responsibility receive timely and relevant information. Information flows both ways through the Fusion Centers. They not only receive information from and distribute it to state and local entities, but also provide information to federal agencies. In effect, Fusion Centers operate as regional data hubs feeding federal, state and local intelligence agencies. A standardized reporting form called a Suspicious Activity

Report ("SAR") is a critical element of the program for handling law-enforcement and intelligence information at Fusion Centers. To ensure that Fusion Centers may carry out their role in an effective way, the PM-ISE adopted a technical standard known as the Information Exchange Packet Documentation ("IEPD") specifically for SARs. ISE Functional Standards for Suspicious Activity Reporting, Version 1.5 (June 2009). The IEPD, like the NIEM and the UCORE, requires open data formats in order to facilitate cross-platform sharing of information.

2. The DNI and ICD 501

170. Second, the IRTPA created the office of the Director of National Intelligence ("DNI") and gave him overall responsibility for the national intelligence community ("IC"). 50 U.S.C § 401, Part 1.3. Currently, the PM-ISE reports to the DNI. Among the DNI's responsibilities is to "develop guidelines for how information or intelligence is provided to or accessed by the Intelligence Community … and for how the information or intelligence may be used and shared by the Intelligence Community." *Id.* Part 1.3(a). The DNI is specifically charged to "establish common security and access standards for managing and handling intelligence systems, information, and products, with special emphasis on facilitating" the "establishment of standards for an interoperable information sharing enterprise that facilitates the sharing of intelligence information among elements of the Intelligence Community." *Id.* Part 1.3(b)(4)(B).

171. In July 2006 and July 2007, respectively, the DNI issued Intelligence Community Directives 301 and 302 ("ICDs 301 and 302") declaring as policy within the IC a commitment to open system capabilities and tools. These directives were followed by Intelligence Community Directive 501 ("ICD 501"). ICD 501 imposes what is called the "responsibility to discover." "IC elements" – agencies within the IC – are charged with "ensur[ing] that new information technology (IT) systems or significant changes to existing IT systems provide the capability for

discovery, dissemination, and retrieval of information collected or analysis produced through automated means." ICD 501 specifically provides that "legacy information," like all other forms of information, must be retrievable and available for dissemination through "automated means."

172. ICD 501 imposes on those within the IC who actually possess information, known as "stewards," a concomitant "responsibility to provide." Stewards must "make all information collected and all analysis produced by an IC element available for discovery by automated means … including information collected through contracts, arrangements, agreements, or understandings. In some cases, this may mean that only standardized or limited metadata is made discoverable. In such cases, discovery requires that such information be described with sufficient detail to allow authorized IC personnel to make a reasonable determination regarding whether it is relevant to a mission need."

173. In carrying out their responsibilities to discover and provide, ICD 501 specifically directs IC agencies to develop the ability to search for information across multiple data sources, and, upon finding information responsive to requests from other IC agencies, to selectively withhold information so that sanitized but useable content may be provided ("multilevel security screening"). Compliance with ICD 501 requires open data format software tools because agencies must have the ability to search and analyze data in multiple data sources, and because, once responsive information is discovered and appropriately redacted as part of the multilevel security screening process, the sanitized data must be freely shareable across enterprise platforms.

B. Palantir has set a new open data format standard in intelligence and law-enforcement software and is the only company to offer tools fully compliant with ICD 501.

174. Palantir is a young, highly innovative company that has rapidly become a leading

provider of enterprise-based software for intelligence and law-enforcement agencies, among other specialized applications. Its customers include a wide variety of federal, state and local government agencies, among them the Los Angeles County Sheriff's Department ("LASD"), the Federal Bureau of Investigation ("FBI"), the Department of Defense ("DOD"), the Defense Intelligence Agency ("DIA"), the U.S. Counter-IED Operations Integration Center ("COIC"), and Fusion Centers, among many others.

175. Palantir pursues a business model utilizing open data formats and is dedicated to ensuring that its software works well and integrates with all other types of software. One component of Palantir is its data integration layer, able to take in data from literally any digitized source to allow for human analysis. This includes any sort of structured/tabular information, typically found in a database system or spreadsheet, as well as unstructured textual information, typically found in word-processing documents, emails, and other forms of written text. A key strength of Palantir's system is its ability to draw upon data from many different sources, allowing analysis, sharing, and use of data in many different formats, whether structured or unstructured.

176. Palantir's software allows its customers to manage, analyze, and, when appropriate, share within the organization or with other entities vast quantities of data and the relational analyses of that data, even if the data has been collected, stored or organized using disparate software systems. As the 9/11 Commission concluded, "[t]he importance of integrated, all-source analysis cannot be overstated." Without the free transferability of data between and among agencies, this critically important policy objective could never be met. Palantir built a software platform utilizing open data formats that meets this technical challenge. For example, Palantir's software is fully compliant with ICD 501. To date, Palantir is unaware of any other company to have developed software tools that are capable of meeting all the demands of ICD

501.

177. Many government customers include explicit requirements for interoperability in work orders and statements of work. For example, a DIA Statement of Work pursuant to a government contract that Palantir has with that agency states as follows: "This project will leverage Palantir Technologies' unique analytical capabilities to respond to priority requirements to provide a system of systems. This project will provide the user an environment for performing intelligence functions consistent with the Intelligence Community Enterprise Architecture. The project includes modernization, standardization of data sources, horizontal integration, all-source analysis and interoperability…."

178. The effectiveness and power of Palantir's software has been well-recognized and has real-world advantages. According to a recent press report in the Wall Street Journal, Palantir's "main advance is a user friendly search tool that can scan multiple data sources at once." Siobahn Gorman, "How Team of Geeks Cracked Spy Trade," Wall Street Journal (September 4, 2009). This capability, the Journal pointed out, permits "an analyst who is following a tip about a planned terror attack … [to] more quickly and easily unearth connections among suspects, money transfers, phone calls and previous attacks around the globe."

C. i2's use of a customer data "lock-in" strategy is an improper attempt to preserve its legacy position in the marketplace.

179. i2, a competitor of Palantir, takes a very different approach to intelligence and law-enforcement software than does Palantir. i2 has been around for decades. It has two principal product lines, one known as Analyst's Notebook ("ANB"), and the other known as Coplink. ANB enables the graphical display of data, but because it is primarily a stand-alone visualization tool, i2 cannot deliver the powerful cross-platform capabilities offered by Palantir's software suite. iBase, a database tool, is part of i2's ANB product line.

180. i2 uses both license restrictions and technical restrictions to obstruct interoperability with the software of competitors, such as Palantir. i2 does this by creating closed file formats not accessible by any non-i2 software, and then using license restrictions to bar competitors from helping customers transfer their accumulated data and analysis into the competing software. Since that data and analysis may be accessed only by launching and running an i2 licensed program, i2 locks in its customers with its license restrictions. i2 further secures this lock-in by requiring a special key inserted in the user's computer, known as a "dongle," to launch ANB, even after the program is already installed on a user's computer. In effect, i2's license and technical restrictions build a wall that prevents free transferability of files coded in i2's closed file format to other software tools.

181. On information and belief, the express terms of many of i2's government contracts require it to permit its government customers to modify, adapt or combine the software it sells to them with other software products used by those customers. In addition, i2's government contracts all include an implied obligation of good faith under which i2 is barred from doing anything to deprive its agency customers of the value of the software delivered to them, or from including any feature in that software that will obstruct or frustrate an agency customer from fulfilling its obligations under federal law.

182. Often, i2's customers find that they cannot by themselves import data files created using i2 software into a form readable by Palantir. They discover that to do that, they need technical guidance and assistance that only Palantir can provide. i2 customers in this position have often requested that Palantir convert data into a format accessible by Palantir's software so that they can preserve and continue to benefit from the legacy value of old data and analyses stored using i2's software. This occurs because customers who have used ANB over long periods of time have generally created many charts using ANB containing data gathered by the

customer, but then saved by the ANB software in a data format carrying the file extension ".anb," a closed format.

183. i2's strategy of locking-in the data and analyses of its government agency customers forces the customers back into the mode decried by the 9/11 Report, where "stove-pipes" of information were common, and "connecting the dots" was a hit-and-miss proposition. To understand why i2's obstruction of the government's interoperability policy is a gravely serious problem, one need only envision a scenario in which special forces on the ground in Iraq or Afghanistan are unable to obtain access to details regarding insurgents in the vicinity due to i2's efforts to lock up the information.

184. i2 is willing to permit transferability of data, so long as it flows into i2's software into a form readable by i2 but not out of i2 into a form readable by Palantir. Long ago, Palantir developed an export tool (a tool that exports data stored using Palantir into a form readable by i2) and only more recently did it develop an import tool (a tool that runs i2's software and then imports data stored using i2 into a form readable by Palantir). Palantir developed portions of the exporter at customer sites using customers' licensed i2 software. The exporter has been widely used by i2's and Palantir's intelligence and defense customers. For example, many DOD end users in the military use ANB on the ground in Iraq and Afghanistan to visualize some of their data. When DOD analysts in the United States use Palantir to analyze the data, an export is necessary to transmit that data to the end users in the field who have access to ANB, but not Palantir. To accomplish the export, Palantir's Forward Deployed Engineers often need to run i2's software, which they have done in the field at the request of troops on the ground.

185. Following its non-proprietary philosophy, Palantir first built that export capability to export data *from* Palantir *into* i2. i2 never complained about the exportation of data from Palantir into a form readable by i2, however, since this furthers its objective of "locking in"

customer data. It was not until several years after Palantir built and demonstrated publicly that it had developed an importer that i2 complained – in the form of this lawsuit. i2 attempted to mask this transparently anticompetitive objective by using the manner in which Palantir allegedly obtained i2 software from SRS as its excuse for complaining, even though for years i2 customers had been making i2 software available to Palantir and even though i2 had long been aware of Palantir's ability to transfer data to or from i2's software. The actual trigger for this lawsuit had nothing to do with SRS. What spurred the lawsuit was Palantir's rapidly growing popularity in the marketplace. Indeed, i2 has sought to use the allegations in its Complaint in this case for improper, non-litigation purposes. Palantir is informed and believes that i2 targeted specific Palantir customers and potential customers and sought to interfere with Palantir's contractual relationships and/or prospective contractual relationships with those customers by presenting to them the false allegations in its Complaint.

186. Just as i2's customers have requested Palantir's assistance transferring data into and out of ANB, i2's customers have also requested that Palantir examine their data stored in i2's iBase schema in order to support their needs for interoperability. Despite the needs of customers for interoperability in both the ANB and iBase product lines, and despite the fact that i2's own customers have asked Palantir to use their licensed i2 software in order to meet those needs, i2 has taken the position that, under contractual restrictions in i2's customer licenses, any intelligence or investigative data or analysis that has been saved using i2's software – or, presumably, might be created in the future in i2's software – is locked in and must be used exclusively with i2's software. As a direct result of i2's strategy, any United States Government or other government intelligence, law-enforcement, homeland security, military, or other agency or user, whether our troops on the ground, intelligence officers in a hostile area, or cops taking down a terrorist cell here at home, that is not using i2, simply cannot benefit from all potentially

life-saving, or otherwise relevant, information.

187. i2's strategy is to hold customers captive by presenting them with a choice: rely exclusively on i2's suite of software tools, with all of their inherent limitations, or adopt Palantir's much more powerful software tool suite at the cost of losing access to accumulated data and years of work in ANB or Coplink – putting the customer's mission at risk. i2 forces that choice on customers by blocking interoperability with Palantir and other competing software vendors. There is no legitimate business purpose for i2's campaign against interoperability with competing vendors. i2's refusal to allow interoperability is driven solely by its desire to preserve its legacy position and stifle innovation in this uniquely important marketplace, even at the expense of our national security.

188. i2's closed data format is just one of dozens of file types with which customers expect Palantir to integrate. On information and belief, Palantir understands that other competitors of i2 have developed or are seeking to develop data export and import functionality into and out of many types of file formats, including i2's. Thus, while Palantir has been the technology leader in enabling compliance with federally-mandated data sharing standards, it has not been alone in responding to the needs of governmental agencies within the ISE and the IC for interoperable systems. Open data formats are required and necessary for compliance with that mandate. Because i2's strategy of locking in its customers' data obstructs the ability of all suppliers of intelligence and law-enforcement software to provide interoperable products that use open data formats – and, more importantly, obstructs government officers from carrying out their missions – its business practices are fundamentally at odds with federal law and policy.

CLAIM FOR DECLARATORY RELIEF

189. Paragraphs 124 through 135 and 157 through 188 are incorporated and realleged here, as if fully set forth.

190. In Paragraph 31 of the Complaint, i2 alleges that its customer license restrictions "ensure that i2's confidential software and related trade secrets and confidential information [are] provided to legitimate licensees only, and [are] not available to third parties – particularly to i2's competitors." Palantir denies that i2's licenses can be lawfully enforced in a manner that blocks i2's customers from making i2's software available for use by Palantir to help its customers achieve interoperability between i2 and Palantir, and vice versa. Because i2 and Palantir have taken these opposing positions, Palantir seeks declaratory relief.

191. To the extent i2's customer license restrictions block and impede i2's competitors from offering government customers software tools that do nothing more than open i2's software applications so that files saved in i2's closed data formats may be imported to and used in other software applications (as well as enabling export from Palantir and other platforms into i2), these license restrictions contravene established federal law and policy. Specifically (i) they are inconsistent with the interoperability requirements set forth in 6 U.S.C. § 485(b)(2), the foundational statute authorizing the creation of the ISE, (ii) they obstruct participants in the ISE – including private sector suppliers – from fully complying with open data format standards promulgated by the ISE-PM under Presidential authority, and (iii) they prevent IC agencies from fully complying with the open data format directives of the DNI, including ICDs 301 and 302, and ICD 501, adopted pursuant to the DNI's statutory authority under 6 U.S.C § 485(b)(6)(B).

192. An actual, justiciable and continuing controversy has arisen between Palantir and i2 as to whether and to what extent it is permissible for Palantir to respond to continuing requests from i2 customers to assist customers in meeting their obligations under federal law to ensure interoperability between the software products used by them. Pursuant to 28 U.S.C. §§ 2201 and 2202, and Federal Rule of Civil Procedure 57, Palantir requests a judicial declaration that, in the case of any agency or other entity that is part of the ISE or the IC,

(a) it is lawful and permissible for any customer of i2 that has lawfully obtained a license from i2 to give Palantir or any other competitor of i2 access to i2's software for the limited purpose of

(i) reading files or other data coded in i2's closed format so that the files or data may be imported into, or exported out of, the competitor's software in accordance with the customer's need for interoperability, or

(ii) developing software tools capable of reading files or other data coded in i2's closed format so that the files or data may be imported into, or exported out of, the competitor's software in accordance with the customer's need for interoperability; and

(b) further, that any clause in any i2 customer license that purports to bar or otherwise restrict the customer from disclosing to a competitor of i2 any licensed information that may be necessary for the i2 competitor to have so that the competitor may ensure that its software products are interoperable with i2's software products, is void and unenforceable.

RESERVATION OF ADDITIONAL REMEDIES

193. Palantir specifically gives notice that it may rely upon such other claims or defenses as may become available by law, or pursuant to statute, or discovery proceedings in this case, and hereby reserves the right to amend its Answer And Counterclaim to assert such defenses and/or claims.

PRAYER FOR RELIEF

WHEREFORE, Palantir prays for judgment and relief as follows:

1. That Plaintiffs take nothing by their Complaint;

2. That the Complaint be dismissed with prejudice;

3. For attorneys' fees and costs of suit;

4. For declaratory relief, as outlined above in the Counterclaim; and

5. For such other and further relief as the Court may deem just and proper.

Dated: October 19, 2010

WILMER CUTLER PICKERING HALE AND DORR LLP

By: */s/*_____

Carl Nichols, VSB No. 43065
D. Bradford Hardin, Jr., VSB No. 76812
1875 Pennsylvania Avenue, NW
Washington, DC 20006
Telephone: (202) 663-6000
Facsimile: (202) 663 6363
Email: Carl.Nichols@wilmerhale.com
Email: Bradford.Hardin@wilmerhale.com

Attorneys for Defendants PALANTIR TECHNOLOGIES, INC., SHYAM SANKAR, and DR. ASHER SINENSKY

Of Counsel:

John W. Keker (*admitted pro hac vice*)
Elliot R. Peters (*admitted pro hac vice)*
Jeffrey R. Chanin (*admitted pro hac vice)*
Jon B. Streeter (*admitted pro hac vice)*
Eugene M. Paige (*admitted pro hac vice)*
KEKER & VAN NEST LLP
710 Sansome Street
San Francisco, CA 94111-1704
Telephone: (415) 391-5400
Facsimile: (415) 397-7188
Email: jkeker@kvn.com
Email: epeters@kvn.com
Email: jchanin@kvn.com
Email: jbs@kvn.com
Email: emp@kvn.com

Attorneys for Defendants PALANTIR TECHNOLOGIES, INC., SHYAM SANKAR, and DR. ASHER SINENSKY

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on the 19th day of October, 2010, a true and correct copy of the foregoing was electronically filed with the Clerk of Court using the CM/ECF system, which will then send a notification of such filing (NEF) to the following:

Robert R. Vieth, Esq.
COOLEY LLP
One Freedom Square | Reston Town Center
11951 Freedom Drive
Reston, VA 20190-5656

Attorney for Plaintiffs i2 Inc. and i2 Limited

Anand Vijay Ramana, Esq.
McGuireWoods LLP (McLean)
1750 Tysons Blvd
Suite 1800
McLean, VA 22102-4215

Attorney for Defendants Nochur Sankar and SRS Enterprises, LLC

I FURTHER CERTIFY that on the 19th day of October, 2010, a true and correct copy of the foregoing was served by hand on the following:

Christopher J. Sundermeier
COOLEY LLP
3175 Hanover Street
Palo Alto, CA 94304-1130

Attorney for Plaintiffs i2 Inc. and i2 Limited

Dated: October 19, 2010

WILMER CUTLER PICKERING HALE AND DORR LLP

By: */s/*_____

Carl Nichols, VSB No. 43065
D. Bradford Hardin, Jr., VSB No. 76812
1875 Pennsylvania Avenue, NW
Washington, DC 20006
Telephone: (202) 663-6000
Facsimile: (202) 663 6363
Email: carl.nichols@wilmerhale.com
Email: Bradford.Hardin@wilmerhale.com

Attorneys for Defendants PALANTIR TECHNOLOGIES, INC., SHYAM SANKAR, and DR. ASHER SINENSKY